ITRC has developed a series of fact sheets that summarize the latest science, engineering, and technologies regarding environmental data management (EDM) best practices. With the complexity of today's environmental organizations' digital infrastructure, no one wants to start over with recreating their infrastructure in case of a disaster. This fact sheet describes best practices to assist the organization's data manager with making disaster recovery as seamless as possible. This fact sheet is intended to give direction for IT data management professionals for implementing the recovery of data.

Additional information related to environmental data management is provided in the ITRC fact sheets on Data Management Planning; Data Governance; Data Lifecycle; Data Access, Sharing, and Security; and Data Storage, Documentation, and Discovery

# 1 INTRODUCTION

As an organization increases the size of its environmental data repository and infrastructure, the need for a disaster recovery plan and implementation increases at the same rate. A data disaster could be a scenario such as a building housing the infrastructure burning down, a server crashing and not coming back online, an employee with critical knowledge about the data environment dying, or other unforeseen situation. It is best practice for an organization to plan for the worst-case scenario. The more complex the organization's infrastructure, the greater the need for an itemized recovery plan. This fact sheet provides a broad step-by-step structure for an organization to follow to assist with the development of a recovery environment. The information in this document can assist the organization regardless of the data management platform used.

# 2 DATA DISASTER RECOVERY PLAN

ITRC guidance document is an easy-to-use, web-based technical and regulatory resource for planning and implementing a data disaster recovery plan. A list of steps in implementing a data disaster recovery plan includes:

- Ensure all data are backed up on a schedule that matches your agency's retention plan.
- Maintain a list of software users and passwords. Some software requires specific administrator users and passwords that are created during installation unless you previously created the users.
- Copy to another location any configuration files saved when setting up the server.
- Maintain copies of links to servers, software installation, and authorizations.
- List all relevant partner agency Representational state transfer (REST) application programming interface (API) connections and any authentication credentials required for access.
- List all data files on the server.
- Make copies of all license files and keys. Store these copies in a secure off-site location.

Some federal granting agencies require an organization to have a secure off-site location for data and the environmental data management system to be compliant with their granting regulations. It is important to understand the requirements of granting agencies to bring a data management solution back online in case of disaster.

# 3 MULTIPLE DATA BACKUP STORAGE SOLUTIONS

When considering a disaster recovery strategy, the following data storage ideas may help an organization recover more quickly:

- Ensure that all install files are stored at an off-site location.
- Ensure that all data backups are performed according to the organization's and granting agency's backup polices.
- Save configuration files and software-specific users and passwords in a secure off-site location.
- Have a document of firewall ports and a step-by-step process for recreating the environment included with the install files that are stored off-site.
- Keep pictures of replication and versioning user connections.

Sometimes the replication and versioning environments can be very complex, with many field workers and data editors and

analysts. Taking screen shots of the environment to know the users and their capabilities beforehand will assist with the redeployment after a data disaster and save valuable time when bringing the organization's environment back online.

# 4 HOW TO PLAN FOR THE WORST

Here are some issues to consider if an organization is planning a disaster recovery strategy:

- Create a list of contacts and their duties for restoring your infrastructure. Keep this list up-to-date with personnel changes.
- Create a step-by-step recovery document. Basically, if there is a question whether an item is critical to the recovery, make copies and store them off site.
- Work with vendors to know the steps that need to be followed to redeploy the organization's data management solution. Each vendor is different, even if they use the same software and development environment.
- If an organization has self-deployed their geospatial data environment, they need to contact their software company for the redeployment procedures for their environment. This will ensure that the environment functions properly when the redeployment is completed.
- If an organization uses a centralized information technology group, work with the group to redeploy the environment according to the software company's deployment procedures.
- The name of the game in disaster recovery is to bring the organization's environment back online as quickly, seamlessly, and painlessly as possible.

# 5 REFERENCES AND ACRONYMS

The references cited in this fact sheet, and the other ITRC EDM Best Practices fact sheets, are included in one combined list that is available on the ITRC web site. The combined acronyms list is also available on the ITRC web site.